Risk Management Plan

Version 2.0.2.

Disability Insurance Automation Phase 3

01/11/07

Revision History

REVISION	DATE OF RELEASE	DIAP3 SHAREPOINT PORTAL SITE REFERENCE #	PURPOSE
1.0.1.	09/10/06		Initial draft release of the plan for review by the DIAP3 project team.
2.0.0.	12/15/06		Total overhaul of content, including updates based upon feedback regarding version 1.0.1. Sent to DIAP3 project team for additional review and approval.
2.0.1.	12/20/06		Incorporated comments from v2.0.0 review. Added Cover page, Revision History, Reviewers, Approvals, and Table of Contents.
2.0.2.	01/11/07		Accepted Changes applied to v2.0.1 and made a few changes based upon review session held 12/21/06.

Reviewers

DOCUMENT REVIEWERS		
Name	**Title**	**Version**
Bob Bradshaw	DIAP3 Co-Project Manager	2.0.2
Linda Fredericksen*	DIAP3 Co- Project Manager	2.0.2
David Rempp	DIAP3 DIB Assistant Project Manager	2.0.1
Bob Laliberte*	DIAP3 Assistant Project Manager	2.0.1
Michelle Bailey	DI Staff	2.0.1
DaMuu Pinckney -Jones	DI Staff	2.0.1
Haitao Zhang	DIAP3 Architect	2.0.1
Jorge C. Muñoz*	DIAP3 Systems Analyst	2.0.1
Darcy Steen	DIAP3 Project Analyst (Document Owner)	2.0.1
Tad Allred	FPD Representative	2.0.1
Sheri Huber	BOPSD Representative – Declined Review	2.0.1
Jeanine Fenton	BOPSD Representative – Declined Review (per Sheri)	2.0.1

* Denotes reviewers who returned a Comments Matrix (regarding v2.0.0) with proposed changes/updates.

Approvals

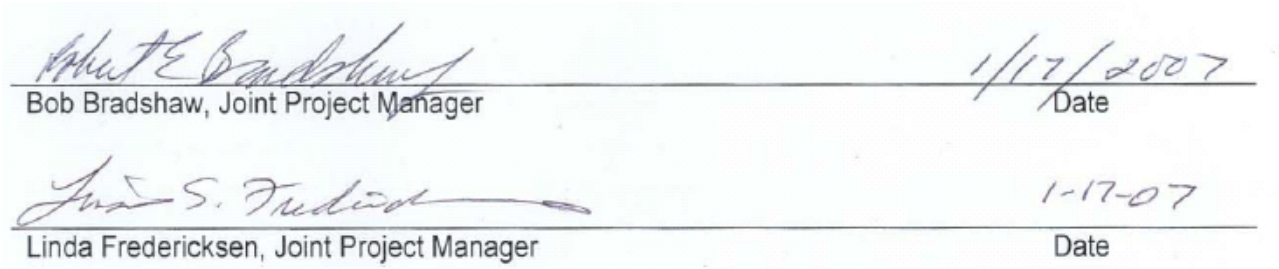


Table of Contents

DIAP3 Risk Management Plan

1. General Information

Information to be provided in this section gives a specific name to the project as well as pertinent information about the personnel involved. (See IT PMM Section 3.8 for more detail)

1.1. Project ID	7100-192	**1.5.** Date	01/11/07
1.2. Project Name	Disability Insurance Automation Phase 3 (DIAP3)	**1.6.** Project Criticality Rating	High
		1.7. Project Sponsor	Sandra Poole
1.3. Controlling IT Div.	TFSD	**1.8.** Project Managers	Bob Bradshaw Linda Fredericksen
1.4. Program Branch	DIB	**1.9.** Author	Darcy Steen

2. Risk Management Methodology

Define the approaches, tools, and data sources used to perform risk management on this project.

2.1. Framework

Risk analysis, risk planning and tracking, and risk escalation are performed in accordance with the Department of Finance/Office of Technology Research, Oversight and Security (DOF/OTROS) IT Project Oversight Framework (ITPOF). The ITPOF can be found as Section 45 of the State Information Management Manual using the following link:
http://www.dof.ca.gov/HTML/IT/SIMM/SIMM.htm

2.2. Methodology

The Risk Manager and all others associated with risk activities will use the EDD IT Project Management Methodology (PMM) for identifying and managing risk. The PMM is compliant with the OTROS ITPOF. The IT PMM may be viewed in its entirety using the following link:
http://eddi.edd.ca.gov/sites/TFSD/PMS/PMO/IT%20PMM/Forms/AllItems.aspx

2.3. Categorization

The IT PMM "Categorization and Examples of Risk" is used to categorize risks. These categories are based on the ITPOF and EDD's IT PMM. Project risks are assigned to one of the following categories:

	Category		Category
2.3.1.	Plan/Schedule	**2.3.10.**	Organization and Management
2.3.2.	User Involvement	**2.3.11.**	Contractor Performance
2.3.3.	Product Characteristics	**2.3.12.**	External Environment
2.3.4.	Design & Implementation	**2.3.13.**	Process
2.3.5.	Financial	**2.3.14.**	System Security
2.3.6.	Legal	**2.3.15.**	Other
2.3.7.	Development Environment	**2.3.16.**	Physical Security
2.3.8.	Requirements Management	**2.3.17.**	Procurement
2.3.9.	Personnel		

2.4. Risk Descriptions

Risk Descriptions will use concise declarations of risk using the following standard notation and sentence structure:

Concern – Likelihood – Consequence

Likelihood refers to the probability that the consequence identified for the risk (concern) will be realized if the risk event occurs. Choices for Likelihood are:

2.4.1. Will almost certainly (>50/50)

2.4.2. Will likely (50/50)

2.4.3. May (<50/50)

(See 9.3.5. for examples)

2.5. Risk Response

Planning focuses on four techniques for developing responses to risk events as follows:

2.5.1. Risk Avoidance – Changing the Project Plan to eliminate the threat of a specific risk event. Although the project team can never eliminate all risk events, some specific risks may be avoided. Creativity is often required to develop risk avoidance strategies.

2.5.2. Risk Transference/Deflection – Seeking to shift the consequence of a risk to a third party via a contract provision with a third party, through an insurance policy, or a vendor warranty. This third party also takes ownership of the risk response. It is important to note that transferring the risk to another party does not eliminate it.

2.5.3. Risk Mitigation – Reducing the probability and/or the consequences of an adverse risk event to an acceptable threshold. It is commonly known that taking early action to reduce the probability of a risk occurring or its impact on the project is more effective than trying to repair the consequences after it has occurred. Mitigation costs should be appropriate, given the likely probability of the risk and its potential consequences.

2.5.4. Risk Acceptance – Risk response strategy that prepares for, and deals with, the consequences of a risk event – either actively (developing a contingency plan) or passively (accepting the consequences). There is no plan on the part of the team to take action on this risk.

2.6. Common Definition of Risk

2.6.1. Risks are considered potential events for which risk planning can occur.

2.6.2. Realized Risk is defined as an identified risk event that has occurred.

2.7. Risks Vs. Issues

Risk Management differs from Issue Management in that:

2.7.1. Risks are events that have not yet occurred and can be planned for.

2.7.2. Issues are events that were not planned for in risk planning, yet they have occurred.

2.7.3. A risk typically will not mature into an issue, and an issue typically will not mature into a risk.

3. Risk Assumptions

Define any initial risk assumptions that are known at the current time. Include any risk factors standard to the performing organization.

3.1. Criticality

The project criticality rating has been established as **HIGH**, and the components of the Risk Management Plan have been developed based upon this rating. It is assumed that this rating will not fluctuate or change, and therefore the requirements for managing risk will not change.

3.2. Risk Mitigation

The DIAP3 Steering Committee, Project Sponsors, and Project Management Team are risk averse and therefore seek to mitigate risk whenever possible. Their primary objective is to minimize or nullify the impact of risk whenever possible; otherwise, they strive to minimize adverse impact to the project and/or to EDD's business. Acceptance of risk events will be kept to a minimum.

4. Roles and Responsibilities

Define the lead, support, and risk management team membership for each type of action in the Risk Plan.

	Role	Responsibility
4.1.	Executive Committee	Provides level 3 (highest) approval authority regarding support and guidance to risks that are caused by events outside the control of the project or the affected branches.
4.2.	Steering Committee	Provides level 2 approval authority. Approves risk event planning and monitors risk status. Reviews formal risk analysis documents when needed.

	Role	Responsibility
4.3.	Joint Project Managers	Provide Level 1 (lowest) approval authority. Perform coordination between program and Information Technology Branch personnel and escalate risk to the Steering and Executive Committees when appropriate. Provide input on risk identification and analysis, mitigation, contingency planning and escalation. Provide direction on specific risk events. Sponsor periodic and continuous risk assessments, mitigation development and implementation, and contingency planning. Respond to risk assessments and findings Is ultimately accountable for risk management on the DIAP3 project, including risk escalation.
4.4.	Project Sponsors	Provide direction and decision-making for project risks. Project Sponsor holds a seat on the Steering Committee.
4.5.	Risk Team	Reviews and approves risk analyses, mitigation/prevention and contingency plans, and monitors action items under its control. Provides updates for risk assessment and tracking. The Risk Team consists of the following members who attend the Biweekly Risk Management meetings: • Joint IT and DI Project Managers • Risk Manager • Risk Owners • Vendor Managers • Any staff deemed necessary for identifying and managing risk
4.6.	Risk Manager	Facilitates overall risk assessment and risk strategy development, assigns risk analysis, distributes analysis results, tracks risk activity and metrics, documents and reports on risk management activities, tracks risk status, and escalates risk events when necessary.
4.7.	Business Risk Lead	Facilitates Business risk assessment and risk strategy development, assigns risk analysis, distributes analysis results, tracks risk activity and metrics, documents and reports on risk management activities, tracks risk status, and escalates risk events when necessary.
4.8.	Vendor Managers	Identify risk whenever they become aware of it and notify the Risk Manager at the earliest possible time. Also, provide expertise and support to the Risk Manager in managing project risks.
4.9.	Project Team	Identifies risk whenever they become aware of it and notifies the Risk Manager at the earliest possible time. Team members also identify and document risks and issues associated with design, build, implementation, and transition to production. They also provide risk analyses as assigned by the Risk Manager and risk tracking updates.
4.10.	Risk Owner	Facilitates the definition of risks for which they are assigned, and maintains ultimate responsibility for ensuring risk activities are executed when necessary. This usually is associated with a subject matter expert in the category of risk that has been assigned. This person usually has control of the resources that will be assigned to work on tasks associated with risk mitigation or execution of the contingency plan. The Risk Owner must: • Know all risks that are assigned to them and keep current on their status • Understand the intent of each risk (Why it was identified and its impact) • Make sure all components for each risk (Impact, probability, etc.) are defined for inclusion in the risk repository • Construct Risk Statement/Description using the required format (see section 2.4) • Perform analysis and document requirements for Mitigation and Contingency Plans, including triggers and time required to implement/perform each aspect of the plans • Come to scheduled risk sessions fully prepared with all of the above information

5. Time Frames

Define the frequency and duration of the risk management process, and when it is performed throughout the project life cycle.

5.1. **Risk Management** – will be performed for the entire duration of the project.

5.2. **Risk Meetings** – At least Bi-weekly, more frequent when warranted.

5.3. **Risk Escalation** – See Section 7

5.4. Risk Reporting – Risks are included in weekly and monthly project Status Reports (See Communication Management Plan)

6. Risk Ranking/Scoring Techniques

Indicate the ranking/scoring method for the type and timing of the qualitative and quantitative risk analysis.

Each risk is ranked for the following:

6.1. Impact

6.1.1. HIGH impact = the risk represents a significant negative impact on project baselines (budget, schedule or scope)

6.1.2. MEDIUM impact = the risk represents a material impact that would significantly affect users, customers or other key stakeholders

6.1.3. LOW impact = the risk does not represent a significant or material impact on project baselines

6.2. Probability of Occurrence

6.2.1. HIGH probability = the risk is almost certain or very likely to occur

6.2.2. MEDIUM probability = the risk may occur or has a 50/50 chance of occurring

6.2.3. LOW probability = the risk is unlikely or probably will not occur

6.3. Exposure

Each Risk receives an ***Exposure*** rating based on a calculation of Impact and Probability using the OTROS Project Oversight Framework's Risk Exposure Matrix. Risk Exposure can be HIGH, MEDIUM or LOW. Risk Exposure is determined for each risk by looking at the intersection of Impact and Probability as shown in the table below. The Exposure rating is used as one of two inputs for determining risk severity.

		Probability		
		High	Medium	Low
Impact	High	**High**	**High**	Medium
	Medium	**High**	Medium	Low
	Low	Medium	Low	Low

Figure 6.3.1 - Risk Exposure Matrix

6.4. Time Frame

6.4.1. SHORT time frame = Time remaining before action must be initiated to implement/execute the Mitigation Plan is less than (<) 6 months

6.4.2. MEDIUM time frame = Time remaining before action must be initiated to implement/execute the Mitigation Plan is 6 months to 1 year

6.4.3. LONG time frame = Time remaining before action must be initiated to implement/execute the Mitigation Plan is greater than (>) 1 year

(See 9.3.15. for examples and more detailed information)

6.5. Severity

Each Risk receives a Severity rating based on a calculation of Exposure and Time Frame using the OTROS Project Oversight Framework's Risk Severity Matrix shown below. Risk Severity can be HIGH, MEDIUM or LOW.

		Exposure		
		High	Medium	Low
Time Frame	Short	**High**	**High**	Medium
	Medium	**High**	Medium	Low
	Long	Medium	Low	Low

Figure 6.5.1 - Risk Severity Matrix

7. Risk Thresholds

Establish the level of authority at which the Project Manager and Project Team may take action without escalation. This should include criteria for risks that are acted upon, by whom, and in what manner. The Project Manager, Customer and Project Sponsor may have different risk thresholds.

Thresholds - Based Upon Severity and Impact to Baselines and Dependent Projects

	Risk Severity*	Impact of Risk to Baselines**/ Dependent Projects	Entity With Approval Authority	Escalation
7.1.	Low	Impact to baselines/ dependent projects is negligible (Variance is < 2.5%)	Joint Project Managers	**Level 1** • Within 2 working days after identification of risk - Any project participant must escalate to the Risk Manager. • Within 1 working day of receipt of Risk form – Risk Manager enters risk into Risk Repository on DIAP3 Sharepoint Site and notifies Joint Project Managers.
7.2.	Medium	Impact to baselines/ dependent projects causes a variance of 2.5% to 5%	Joint Project Managers/ Steering Committee	**Level 2** • Within 2 working days after identification of risk - Any project participant must escalate to the Risk Manager. • Within 1 working day of receipt of Risk form – Risk Manager enters risk into Risk Repository on DIAP3 Sharepoint Site and notifies Joint Project Managers. • Within 2 working days after being notified of risk, the Joint Project Managers notify Steering Committee. The Steering committee can perform assessment and determine recommendations either at their regularly scheduled monthly session or a special session can be convened (depending on Time Frame of risk).
7.3.	High	Impact to baselines/ dependent projects causes a variance that is > 5%	Executive Committee	**Level 3** • Within 2 working days after identification of risk - Any project participant must escalate to the Risk Manager. • Within 1 working day of receipt of Risk form – Risk Manager enters risk into Risk Repository on DIAP3 Sharepoint Site and notifies Joint Project Managers. • Within 2 working days after being notified of risk, the Joint Project Managers notify Steering Committee. The Steering committee can perform assessment and determine recommendations either at their regularly scheduled monthly session or a special session can be convened (depending on Time Frame of risk). • As soon as Steering Committee assessment and recommendations are complete, the Joint Project Managers notify the Executive Committee. The Executive committee can perform assessment and determine recommendations either at their regularly scheduled quarterly session or a special session can be convened (depending on Time Frame of risk).

* Severity requirements are based upon the Risk Escalation Matrix contained in the OTROS ITPOF.

** Baselines are established for Scope, Schedule (milestone phase end date) and Cost).

When applying thresholds, if escalation requirement levels differ between Severity vs. Impact, then the higher of the two escalation level requirements must be followed.

8. Risk Communications

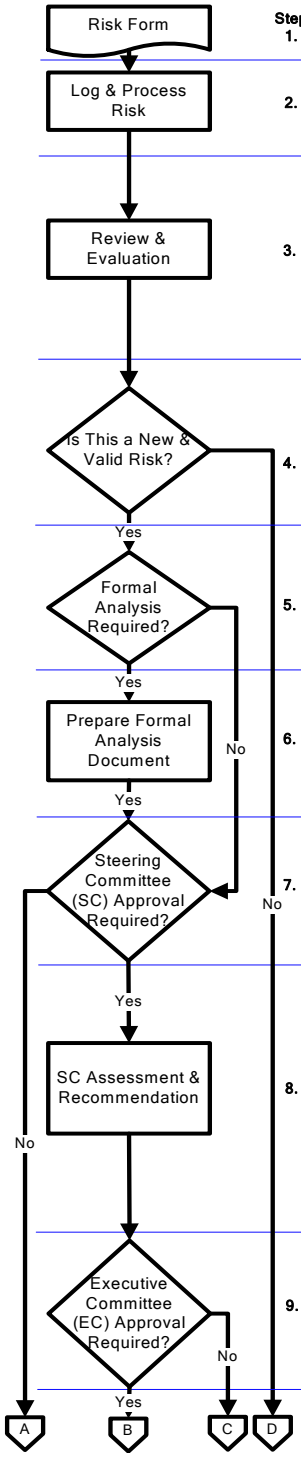
Define how the results of the risk management processes are documented, analyzed, and communicated to the project team, internal and external stakeholders, sponsors, and others.

Please reference the Communication Management Plan for details on how risk communications will be addressed.

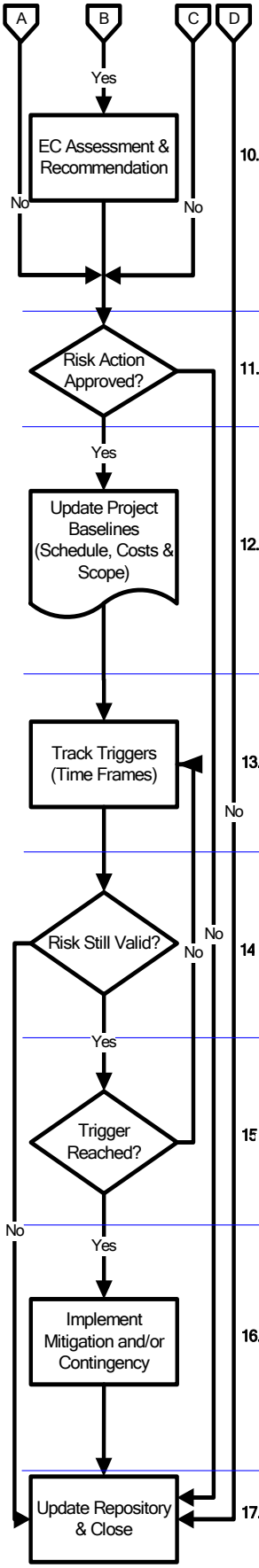
9. Risk Tracking Process

Document how all facets of risk activities are recorded for the benefit of the current project, future needs, and lessons learned.

9.1. Risk Identification, Tracking and Implementation



Step		
1.	Stakeholder	Completes Risk Management Form per instructions on form (See Attachment A).
		Submits completed Risk Management Form to the Risk Manager.
2.	Risk Manager	Logs Risk Management Form information into the Risk Repository (which assigns a unique identifier) and makes the appropriate opening entries.
		Notify Risk Owner that a new risk has been identified (cc Joint Project Managers)
3.	Joint Project Managers (JPM)	Reviews and determines validity of risk. Verifies escalation requirements based upon Severity and Impact to baselines/dependent projects and acts accordingly. Level 1: Joint Project Managers retain control of risk disposition. Level 2: Requires escalation to Steering Committee. Level 3: Requires escalation to Steering committee, and then to Executive Committee.
	Risk Manager	Reviews risk in conjunction with the Joint Project Managers.
	Risk Owner	Reviews risk in conjunction with the Joint Project Managers.
	Risk Team	Reviews risk in conjunction with the Joint Project Managers.
4.	**YES**	
	JPM	Go to Step 5, *Decision Point – Formal Analysis Required?*
	NO	
	JPM	Updates Risk Tracking and Risk Resolution sections of the Risk Management Form. Sign-off fields should be completed.
		Forwards completed documents to the Risk Manager. Go to Step 17, *Update Repository & Close.*
5.	**YES**	
	JPM	Go to Step 6, *Prepare Formal Analysis Document.*
	Risk Owner	Go to Step 6, *Prepare Formal Analysis Document.*
	NO	
	JPM	Go to Step 7, *Steering Committee (SC) Approval Required?*
	Risk Owner	Go to Step 7, *Steering Committee (SC) Approval Required?*
6.	JPM	Works with Risk Owner to assign analyst(s) to conduct a formal risk analysis and establishes a due date.
	Risk Owner	Identifies skills needed to complete analysis and assigns resources accordingly.
	EDD Analyst	Prepares the formal Risk Analysis document.
		Submits the completed Risk Analysis document to the JPM and Risk Owner no later than the established due date.
7.	**YES**	
	JPM	Go to Step 8, *SC Assessment & Recommendation.*
	Risk Owner	Go to Step 8, *SC Assessment & Recommendation.*
	NO	
	JPM	Go to Step 11, *Risk Action Approved?*
	Risk Owner	Go to Step 11, *Risk Action Approved?*
8.	JPM	To initiate review – Forwards Risk Management Form and all pertinent documentation to the SC Chairperson. Requests for risk discussion to be added to Steering Committee meeting Agenda. If Special session is necessary, notify project manager to make arrangements.
		If Special session is necessary, notify project manager to make arrangements.
	Risk Manager	If necessary, schedules special session of the Steering Committee.
	Steering Committee (SC)	Reviews the analytical findings and determines whether the Risk concerns are valid and that assessments regarding risk components (Impact, Probability, Time Frame, Mitigation Plan, Contingency Plan, etc.) are accurate, and if so, how risk activities should proceed.
	JPM	Updates Risk Tracking and Risk Resolution sections of the Risk Management Form. Sign-off fields should be completed.
9.	**YES**	
	SC	Go to Step 10, *EC Assessment & Recommendation.*
	NO	
	SC	Go to Step 11, *Risk Action Approved?*



10.	JPM	To initiate review - Forwards Risk Management Form and all pertinent documentation to the EC chairperson. An additional blank copy of the Risk Management Form should be included as part of the package so the EC can document their findings. Specify desired due date for decision & return of documents.
	EC	Reviews the analytical findings and determines whether the Risk concerns are valid and that assessments regarding risk components (Impact, Probability, Time Frame, Mitigation Plan, Contingency Plan, etc.) are accurate, and if so, how risk activities should proceed.
	JPM	After EC review - Enters the final review results onto the Risk Management Form in the section titled "Risk Assessment".
		Submits the completed Risk Management Form to Risk Manager by due date.
11.	**YES**	
	JPM	Go to Step 12, *Update Project Baselines (Schedule, Costs & Scope).*
	NO	
	JPM	Go to Step 17, *Update Repository & Close.*
12.	JPM	If Executive Committee review was performed - Informs SC about the disposition of the risk. If the SC requests an additional meeting for discussion, inform the Risk Manager so the appropriate arrangements can be made.
	Risk Manager	If necessary, schedules meeting with SC.
	SC	If necessary, meets to discuss final disposition of change request.
	JPM	Determines how the implementation will be executed and then updates Project Schedule, Scope Statement and Cost Detail if needed.
		Forwards updated Risk Management form, with impact analysis and all related documents, to the Risk Manager.
	Risk Manager	Reconciles risk records and repository.
13.	Risk Manager	Tracks triggers as documented to ascertain whether they have occurred or not.
		Informs Joint Project Managers about the disposition of the risk. If the JPM requests an additional meeting for discussion, the Risk Manager will make the appropriate arrangements.
	Risk Owner	Tracks triggers as documented to ascertain whether they have occurred or not.
		Notifies Risk Manager if trigger event/date has been reached.
	JPM	Monitors risk status via project status reports, etc. and attends risk sessions.
14	**YES**	
	Risk Manager	Go to Step 15, *Trigger Reached?*
	Risk Owner	Go to Step 15, *Trigger Reached?*
	JPM	Go to Step 15, *Trigger Reached?*
	NO	
	Risk Manager	Go to Step 17, *Update Repository & Close.*
	Risk Owner	Go to Step 17, *Update Repository & Close.*
	JPM	Go to Step 17, *Update Repository & Close.*
15	**YES**	
	Risk Manager	Go to Step 16, *Implement Mitigation and/or Contingency.*
	Risk Owner	Go to Step 16, *Implement Mitigation and/or Contingency.*
	JPM	Go to Step 16, *Implement Mitigation and/or Contingency.*
	NO	
	Risk Manager	Go to Step 13, *Track Triggers (Time Frames).*
	Risk Owner	Go to Step 13, *Track Triggers (Time Frames).*
	JPM	Go to Step 13, *Track Triggers (Time Frames).*
16.	Risk Manager	Informs JPM & Risk Owner that action needs to be taken.
		Updates Risk Repository as task activity progresses.
	JPM	Initiate execution of Mitigation or Contingency Plan.
	Risk Owner	Works with JPM to identify appropriate resources needed and facilitates the completion of the required tasks.
	EDD Analyst	Identifies target completion date and notifies Risk Owner, Risk Manager & JPM.
		Implements mitigation or contingency task(s).
		Documents how and when the task was accomplished by making entries in the Risk Tracking section of the Risk Management Form.
		Returns all completed documents to the Risk Manager.
17.	Risk Manager	Updates Risk Management Form if needed.
		Posts closing entries to the Risk Repository at DIAP3 Sharepoint Site.
		Notifies the author of the Risk Management Form.
		Archives all pertinent documents.

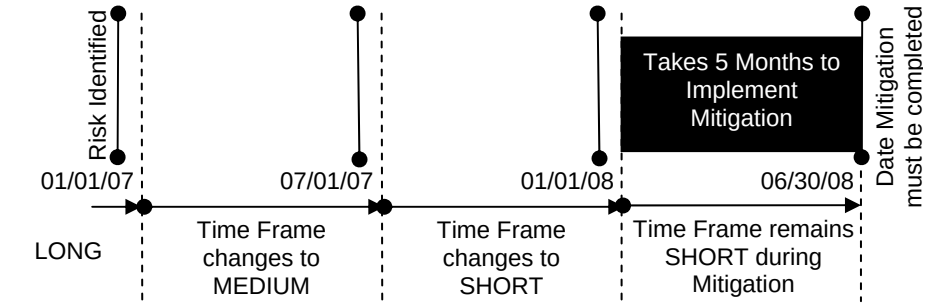
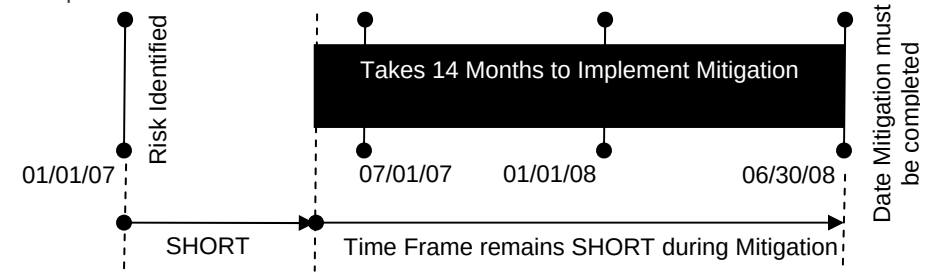
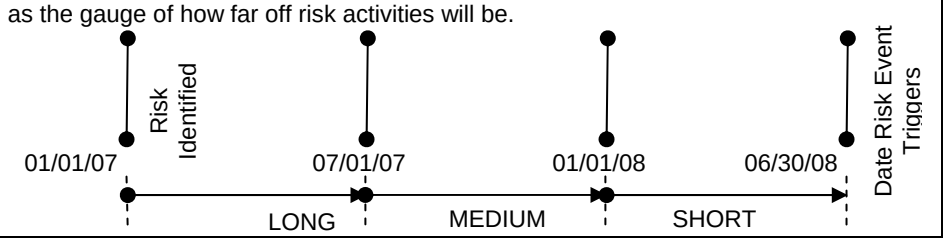
9.2. Risk Meeting Process Overview - based upon a cycle where risk meetings are held bi-weekly

WEEK	DAY OF WEEK	WHO	ACTION TAKEN
OFF-WEEK / NO MEETING HELD	Monday through Thursday	Project Manager/Staff	• Submit new risks. • Submit updates to existing risks.
	Monday through Thursday	Risk Manager	• When new risks or updates are received, make updates to: o Risk repository on DIAP3 SharePoint Site o Update Tracking Document (Header reflects day request was made)
	Friday	Risk Manager	• Send out request (email) for updates. Should include the following information: o Response Due Date (Close of Business Tuesday, week of the meeting) o Current Open Risk List o Current Closed Risk List o Update tracking Document (Log of all updates) Note: cc primary and back-up risk analysts assigned to the engagement.
WEEK MEETING HELD	Monday Through Thursday	Project Manager/Staff	• Submit new risks per Request for Updates. • Submit updates to existing risks per Request for Updates.
	Wednesday (AM)	Risk Manager	• Input updates that have been received from the Request for Updates email into the risk repository. • If any new risks are submitted, initiate escalation process if needed. • Record changes to the risk repository on the Update Tracking document. • Send out pre-meeting email. Should include the following information: o Current Active Risk List o Current Closed Risk List o Update Tracking document (Log of all updates) • Note: Meeting participants are instructed to print their own copy of the documents and bring to the meeting.
	Wednesday through Thursday	Project Manager/Staff	• Print copies of documents received in pre-meeting email.
	Thursday	Project Manager/Staff	• Attend risk meeting (bring copies of documents).
	Thursday	Risk Manager	• Conduct risk meeting.
	Friday	Risk Manager	• Input updates that were captured in the meeting into the risk repository. • If any new risks are submitted, initiate escalation process if needed. • Record changes in the Update Tracking document. • Send out post-meeting email. Should include the following information: o Current Active Risk List o Current Closed Risk List o Update Tracking document (Log of all updates) • Send email reminders to each participant that has action items from the meeting

9.3. Risk Data Fields

The following table provides a description of the fields stored in the Risk Repository on the DIAP3 SharePoint Site:

	Field Name	Description	
9.3.1.	Risk ID	Assigned by the Risk Repository. No entry is required.	
9.3.2.	Status	Open	Possibility of risk event occurrence still exist and requires monitoring/tracking
		Closed	Possibility of risk event occurrence no longer exists
9.3.3.	Risk Event Title	Short, clear, and concise description that defines the risk.	
9.3.4.	Cross Ref. To Change Req. ID/Title	If a Change Request is generated to enact change due to an identified risk, then the Identification/Title should be cross referenced since activities towards its completion should also be tracked as part of the risk resolution.	
9.3.5.	Risk Statement/ Description	Provides a more detailed declaration of the risk description provided in the Risk Event Title. The description should be constructed using the following standard notation and sentence structure: Concern – Likelihood – Consequence. Standard notations to be used for Likelihood are:	
		Will almost certainly	Greater than 50/50 chance of likelihood
		Will likely	50/50 chance of likelihood
		May	Less than 50/50 chance of likelihood
		Examples of typical risk statements include: • Mandated unrealistic implementation date • will almost certainly • lead to significant missing functionality in the implemented system. • Late contractor deliverables • will likely • result in delayed pilot testing. • Regulation changes • may • result in the need for costly change orders and/or delayed implementation.	
9.3.6.	Risk Context/ Analysis (Trigger)	Provides further elaboration regarding the risk that is not part of the Risk Statement/Description. At a minimum, the Risk Trigger should be defined. The trigger (date, event, condition or task) identifies when the risk will most likely occur. You must be able to quantify/measure it.	
		Example of Risk Trigger: • Risk – Personnel most qualified to perform work is unavailable o Trigger - Staff Acquisition Process task begins	
9.3.7.	Originator	Name of individual who initially identifies and documents the risk.	
9.3.8.	Origination Date	The date on which the risk was originally identified and documented.	
9.3.9.	Risk Owner	Name of the project team member that has the ultimate responsibility for ensuring risk activities associated with the risk are executed when necessary. This usually is associated with a subject matter expert in the category of risk that has been assigned. This person usually has control of the resources that will be assigned to work on tasks associated with risk mitigation or execution of the contingency plan.	
9.3.10.	Assigned To	Resource that will be assigned to physically work on tasks associated with risk mitigation or executing the contingency plan.	
9.3.11.	Exposure	Exposure rating is assigned by the Risk Repository. The rating is derived based on a calculation of Impact and Probability using the OTROS Project Oversight Framework's Risk Exposure Matrix. The Exposure rating is used as one of two inputs for determining risk severity. Risk Exposure values are:	
		High	
		Medium	
		Low	
9.3.12.	Severity	Severity rating is based on a calculation of Exposure and Time Frame using the OTROS Project Oversight Framework's Risk Severity Matrix. Risk Severity values are:	
		High	
		Medium	
		Low	

	Field Name	Description	
9.3.13.	Impact	Impact rating is established by project team subject matter experts to indicate the level of impact a documented risk will have on the project. Values are:	
		High	The risk represents a significant negative impact on project baselines (budget, schedule, or scope)
		Medium	The risk represents a material impact that would significantly affect users, customers or other key stakeholders
		Low	The risk does not represent a significant or material impact on project baselines
9.3.14.	Probability	Probability rating is established by project team subject matter experts to indicate the probability (likelihood) that the documented risk event will actually occur. Probability values are:	
		High	The risk is almost certain or very likely to occur
		Medium	The risk may occur or has a 50/50 chance of occurring
		Low	The risk is unlikely or probably will not occur.
9.3.15.	Time Frame	Time Frame rating is established by project team subject matter experts to indicate the time remaining before action must be initiated in order to successfully implement/execute the Mitigation Plan. The remaining time should be calculated by identifying the cut-off (drop-dead) date for when the Mitigation Plan must be fully implemented (the project schedule can assist in making this determination) and subtracting out the length of time required to implement the Plan. Time Frame values are:	
		Short	Time remaining before action must be initiated to implement/execute the Mitigation Plan* is less than (<) 6 months
		Medium	Time remaining before action must be initiated to implement/execute the Mitigation Plan* is 6 months to 1 year
		Long	Time remaining before action must be initiated to implement/execute the Mitigation Plan* is greater than (>) 1 year
		Example 1: 	
		Example 2: 	
		Example 3: Note: *If the risk strategy is Acceptance/Contingency (no mitigation possible), then the anticipated trigger date for the risk event to occur should be used as the gauge of how far off risk activities will be. 	

	Field Name	Description	
9.3.16.	Risk Category	Project risks are assigned to one of the following categories:	
		Plan/Schedule	
		Organization and Management	
		Development Environment	
		User Involvement	
		Contractor Performance	
		Requirements Management	
		Product Characteristics	
		External Environment	
		Personnel	
		Design and Implementation	
		Process	
		Physical Security	
		Financial	
		System Security	
		Procurement	
		Legal	
		Other	
9.3.17.	Risk Response Strategy	There are four strategies for responding to risk:	
		Avoidance	Changing the Project Plan to eliminate the threat of a specific risk event. Although the project team can never eliminate all risk events, some specific risks may be avoided.
		Transference/ Deflection	Seeking to shift the consequence of a risk to a third party via a contract provision with a third party, through an insurance policy, or a vendor warranty. This third party also takes ownership of the risk response. It is important to note that transferring the risk to another party does not eliminate it.
		Mitigation	Reducing the probability and/or the consequences of an adverse risk event to an acceptable threshold. It is commonly known that taking early action to reduce the probability of a risk occurring or its impact on the project is more effective than trying to repair the consequences after it has occurred. Mitigation costs should be appropriate, given the likely probability of the risk and its potential consequences.
		Acceptance/ Contingency	Risk response strategy that prepares for, and deals with, the consequences of a risk event – either actively (developing a contingency plan) or passively (accepting the consequences). There is no plan on the part of the team to take action on this risk.
9.3.18.	Mitigation/ Prevention Plan	Detailed description of the strategy/plan for reducing the probability and/or consequences of an adverse risk event to the project's acceptable thresholds.	
9.3.19.	Contingency Plan	Detailed description of the strategy/plan for preparing for, and dealing with, the consequences of an adverse risk event.	
9.3.20.	Risk Tracking	As change or action is applied to an identified risk, entries are documented to create an audit trail of all activity taken.	
9.3.21.	Final Resolution	Description of the steps taken, or the events that have transpired, that allow for a risk to be closed.	
9.3.22.	Affected Tasks	Tasks that are impacted by this risk.	
9.3.23.	Triggers	Tasks that are triggers for this risk.	
9.3.24.	Mitigation Tasks	Tasks that are part of the mitigation plan.	

	Field Name	Description
9.3.25.	Contingency Plan Tasks	Tasks that are part of the risk contingency plan.
9.3.26.	Linked Risks	Other related risks in this project.
9.3.27.	Linked Issues	Issues that are related to this risk.
9.3.28.	Linked Documents	Project documents that are related to this risk.

The Risk Management Form shown in Appendix A is the tool used to submit and escalate risks. Copies of the form are available at:

Electronic Copy: DIAP3 SharePoint Site, Standard Templates, Risk Management Form
Hard Copy: Can be obtained from the Risk Manager

Appendix A – Risk Management Form – (Manual Entry)

Figure 1: Manual Entry Risk Management Form

Risk Management Form

Risk Management Form		
Probability:	Project: Disability Insurance Automation Phase 3	
Impact:	Risk Title:	
Time Frame:	Originator:	Origination Date:
Severity:	Assigned to:	Report Date:
Risk Assessment		
Risk Statement: *Statement: Provide a more detailed declaration of the risk that was captured for the Risk Title. The risk statement should be constructed using the following standard notation and sentence structure: Concern – Likelihood – Consequence.* *Standard notations to be used for Likelihood are "Will almost certainly" (Greater than 50/50 chance of likelihood), "Will likely" (50/50 chance of likelihood) or "May" (Less than 50/50 chance of likelihood).* *Description: If further detail is needed to document the intent of the risk, you may add an additional description after the Risk Statement sentence to meet this need.*		
Risk Context/Analysis: Risk Owner: Identify the owner organization and individual if possible. Trigger: Identify the event date or condition that is to be used as the indicator for when Mitigation and/or Contingency activities must commence. Risk Category: Identify which category (out of the list of 18) is most applicable. Note: Refer to Section 9.3 for a detailed list of all risk data fields that should be included if applicable.		
Risk Planning		
Strategy: ___Avoidance ___Transference/ Deflection ___Mitigation ___Acceptance/ Contingency	Action Items Mitigation Plan: Identify actions that can be taken to reduce the probability and/or the consequences of an adverse risk event to an acceptable threshold. Contingency Plan: Identify the risk response strategy that prepares for, and deals with, the consequences of a risk event.	
Risk Tracking		
Event/Action/Commitment: Record action taken to implement action items listed above. Before risk closure can occur, final resolution must also be recorded here.		
Risk Resolution - Each escalation level has an entity with approval authority; See Section 7 of Risk Management Plan		
Sign-off:	Sign-off:	Sign-off:
Sign-off Date:	Sign-off Date:	Sign-off Date: